“ENHANCED SECURE SECRET SHARING SCHEME FOR VISUAL CRYPTOGRAPHY”

A

Research Synopsis / Proposal

Submitted to

Swami Ramanand Teerth Marathwada University,

Vishnupuri, Nanded

स्वामी रामानंद तीर्थ मराठवाडा विद्यापीठ, नांदेड.

in partial fulfillment for the Registration of the degree, Doctor of Philosophy in Computer Science (Faculty of Computer Science & Technology)

Submitted By

Mr. A. B. Alde
School of Technology, S.R.T.M. University Nanded, Sub-Center, Peth, Latur

Under the guidance of

Dr. Vikas T. Humbe
Ph.D., MIEEE, FIAET
Assistant Professor,
School of Technology,
Swami Ramanand Teerth Marathwada University,
Sub-Centre, Ausa Road, Peth, Latur, (MS) 413512.

March - 2022

Table of Contents

Abstract of proposed work plan / problem: 1

1. Introduction: 2

2. Review of Literature and Development in the subject (Previous work done in the relevant area): 4

3. Objectives of Research/ Proposed Hypothesis: 6

4. Methodology to be adopted: 7

5. Importance of study / Society application: 11

- **International status. 11**
- **National Status 11**
- **Significance of the study 11**

6. Proposed work Plan/ Formulation and Structure of Study: 12

7. References: 13

“ENHANCED SECURE SECRET SHARING SCHEME FOR VISUAL CRYPTOGRAPHY”

Abstract of proposed work plan / problem:

“Obscuring the important message before disseminating becomes obligatory”. In recent period of time, transmitted data over the internet is unsecure as well as unreliable. A Visual cryptography (VC) or so-called Visual Secret Sharing(VSS) is a new way of cryptography used to encrypt an image (or text image) into n number of parts called Shares that can, then transmitted securely through any communication channels towards different n participants. At the receiver side, secrete image can only be decrypted without any computation when all n number of Shares superimposed together. Hence the decryption is a computation-free decoding process and performs by human visual system without any algorithmic process that provides high security. Visual cryptography is specially designed for data security or providing more secure method for allowing access to more sensitive data. It simply used for user authentication for providing access to data.

Recently many Secrets Sharing Scheme of visual cryptography schemes are developed ranging from (2, 2) Visual Cryptography Scheme to Segment based Visual Cryptography Scheme, Halftone Visual Cryptography to Progressive Multi-resolution Visual Cryptography. But there are so many problems of visual cryptography such as pixel expansion, alignment problem, extensive codebook design, Cheating Prevention, Flipping Issues, Distortion Problem, Thin Line Problems and lossy recovery are quiet unresolved.

Our proposed methodology suggested a way to encrypt, decrypt and also provides double security to the encrypted image. We encrypt an image into two shares. Out of two encrypted Shares, we split-up the Share 2 into number of Cells and then Shuffle all Cells with key generation. Send all Shares with key towards participant side. Participant use key to rearrange all shuffled Cells to its original Share 2 form in proper order. At last participant reveals the original image without any distortion and without any computation when these two Shares are superimposed one another.

1. Introduction:

In recent days, security is a big threat in the transmission medium due to the development of the Internet and multimedia contents such as audio, image, video etc. For transmitting secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed which gave rise to new technologies in the area of Image Cryptography which would require less computation and less storage.

The encryption and decryption are the two techniques used to secure data of any type. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text). Decryption is the process of converting cipher text back to plaintext. There are two types of encryption in widespread use today are symmetric and asymmetric encryption. Encrypting, decrypting, and hashing are the three basic operations in cryptography. Cryptography is the science of protecting information by transforming it into a secure format. It aims at ensuring high end communication between the sender and receiver without any loss of information **(1)**. In this technique, the secret message has become a disordered code after being encrypted and, then it can be transmitted securely via internet. Subsequently, it is recovered by using a correct key. However, one of the flaws of this technique is that encryption and decryption process certainly consume much time **(2) (3)**.

Cryptography is the study of concepts like encryption, decryption, used to provide secure communication, whereas encryption is the process of encoding a message with an algorithm. Now a day's cryptography is widely used in everyday life for authentication, digital signature, electronic money transfer, during secure network communication, for banking transactions cards, computer passwords, and e- commerce transactions etc

Furthermore in cryptography two schemes have been merged such as Secret Sharing Scheme (SSS) and Visual Cryptography (VC). Secret Sharing is a simple cryptographic technique suggested by Blakely **(4)** and Shamir **(5)** as solution to the problem of key management. The secret sharing scheme permits a dealer to split a secret into n shares and distribute them among different n participants. Therefore, the qualified set of participants can recover the secret while the forbidden set can obtain no information about the secret **(6)**. Thus the need of secret sharing can be illustrated in two points; the first is the secret sharing that

gives a tight control and features a single vulnerable point and, the second is that an individual key holder cannot modify or access the data.

Visual Cryptography (VC) is an encryption technique on images (or text, written material, etc.) in which decryption is done by human visual system (HVS) without using any complex computation **(7) (8)**. VC scheme is new direction of the Cryptography and is considered as a subset of secret sharing. To the general secret sharing problem, the Visual Secret Sharing (VSS) acts as a special approach and the secret is a concealed image **(9)**. In this technique, an image is encrypted into number of pieces (known as shares). When the printed shares are physically superimposed together, the image can be decrypted with human vision as shown in Fig.1 below.

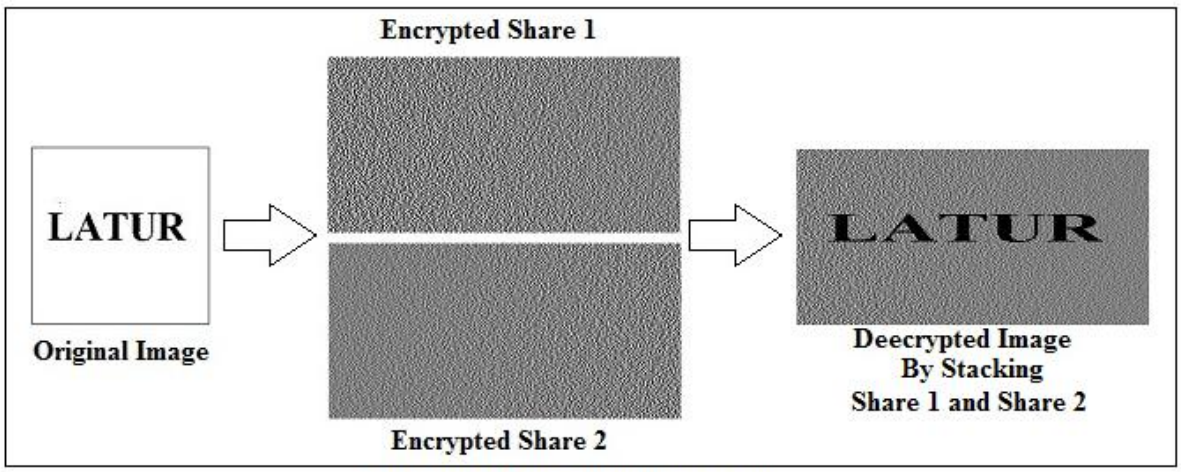

Fig 1 :- Visual Cryptography Scheme

As kind of special secret sharing technology, Visual Cryptography (VC) was introduced by Naor and Shamir in the Eurocrypt'94 **(9)**. This technique does not require any key management nor does it require any algorithm for decryption. Most of these studies, however, concentrate on binary images; few of them proposed methods for processing gray-level and color images. Most of the techniques which are employed on color images such as do not give the original image back. The quality of the generated images is not same as the original and there is lot of loss in the picture quality.

2. Review of Literature and Development in the subject (Previous work done in the relevant area):

Black and White Visual Cryptography Schemes:

Sharing Single Secret

Naor and Shamir's (Moni Naor and Adi Shamir, 1995) **(9)** proposed encoding scheme to share a binary image into two shares Share1 and Share2. Here each share pixel p is encoded into two white and two black pixels each share alone gives no clue about the pixel p whether it is white or black. Secret image is shown only when both shares are superimposed. The disadvantage of the above schemes is that only one set of confidential messages can be embedded, so to share large amounts of confidential messages several shares have to be generated.

Sharing Multiple Secrets

Wu and Chen (Wu and Chen, 1998) **(10)** were first researchers to present the visual cryptography schemes to share two secret images in two shares. They hidden two secret binary images into two random shares, namely A and B, such that the first secret can be seen by stacking the two shares, denoted by A and the second secret can be obtained by first rotating A Θ anti clockwise. They designed the rotation angle Θ to be 90. However, it is easy to obtain that Θ can be 180 or 270

Color Visual Cryptography Schemes:

Sharing Single Secret

Until the year 1997 visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg (Verheul and Tilborg, 1997). **(11)** But the shares generated were meaningless. For sharing a secret color image and also to generate the meaningful share to transmit secret color image Chang and Tsai (Chang *et al*., 2000) anticipated color visual cryptography scheme.

For a secret color image two significant color images are selected as cover images which are the same size as the secret color image. Then according to a predefined Color Index Table, the secret color image will be hidden into two camouflage images. One disadvantage of this scheme is that extra space is required to accumulate the Color Index Table.

Sharing Multiple Secrets

Tzung-Her Chen *et al*. (2008) **(12)** anticipated a multi-secrets visual cryptography which is extended from traditional visual secret sharing. The codebook of traditional visual secret sharing implemented to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by stacking two of share images in a way of shifting. This scheme can be used for multiple binary, gray and color secret images with pixel expansion of 4.

Image encryption based on Cell Shuffling or pixel rotation

Chandra Prakash Singer, Jyoti Bhaarti and R.K. Pateriya (2017) works on cell shuffling and scanning technique for image encryption. They proposed a method which contains two stages. First divide the image into number of blocks and then shuffled the original image and in second stage the spiral wave scan pattern are applied to get encrypted image **(13)**.

Kalyan Das, Aromita Sen and Samir Kumar Bandyopadhyay (2016) develop a method which gives a way out of color image cryptography without any loss and pixel expansion. For this they used sliding puzzle technique in which every block of image is used as a puzzle block and need to be arranged in an orderly manner **(14)**.

Guru Prasad M. Bhat and Nyana G. Bhat (2017) provide the information regarding information security by using Visual Cryptography Scheme by making use of exclusive new technique of splitting of images along with their pixels rotation with the help of generated random number that made an attempt to overcome some of the disadvantage of preexisting techniques of encryption and decryption **(15)**.

Review based on types of Visual Cryptography

Young-Chang Hou **(16)** works on Color visual cryptography and proposes three methods for visual cryptography of gray-level and color images based on past studies in black and white visual cryptography, the halftone technology, and the color decomposition method. Their method retain the advantages of black-and-white visual cryptography, which exploits the human visual system to decrypt secret images without computation, and also have the backward compatibility with the previous

results in black-and-white visual cryptography, such as the t out of n threshold scheme.

Mahmoud E. Hodeish and V.T. Humbe (2014) presents a descriptive review for Visual Cryptography, which covers the "State-of-the-art" concept and classified various schemes **(17)**.

3. Objectives of Research / Proposed Hypothesis:

This research proposal is mainly designed to provide efficient solution to Visual cryptography (VC) for image and various problems such as distortion, pixel expansion, flipping issues and thin line problem. This research also helps to solve the problem related to information security and cipher image transmission.

Objectives of this research proposal are:

1. To provide the more accurate and efficient solutions to various problems with different challenges that are occurred during the Visual Cryptography.
2. To design and implement a novel integrated approach in Visual Cryptography Scheme in order to secure an image transmission.
3. To overcome the problems such as distortion, pixel expansion, flipping issues and thin line problem and improvement in picture quality.
4. To evaluate and analyze the performance of proposed scheme to clarify the quality and efficiency of final produced image in comparison to existence schemes and finally contribute in recommendation and assumption for the future development.

4. Methodology to be adopted:

Proposed research will processed by adopting following methodology:

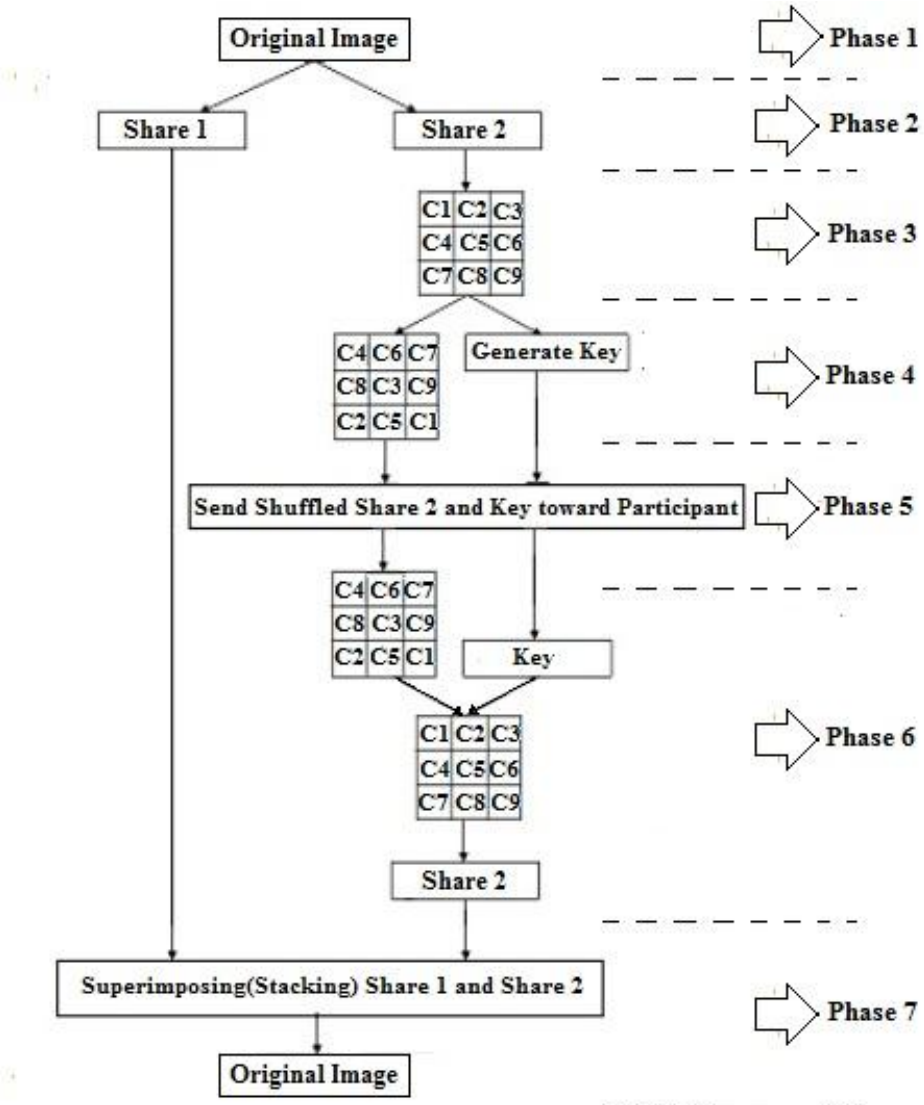

Fig.2:- Praposed Research Methodology

Proposed Research Methodology involves following Phases / Steps……..

Phase 1:- Original image / Convert letter into Image.

Phase 2:- Splitting Original Image into Encrypted Share 1 and Share 2.

Phase 3:- Convert Encrypted share 2 into Cells.

Phase 4:- Shuffle the Cells of Share 2 and Generate Key.

Phase 5:- Send encrypted Cell Shuffled Share 2 and Key towards Participants.

Phase 6:- Rearrange all Shuffled Cells in sequence to form Share 2 by using Key.

Phase 7:- Superimpose Transparencies of Share 1 and Share 2 to reveal Original Image.

The proposed research is focused on developing accurate and secure Visual Cryptography and also focuses on hiding or revolving securing information. While transmitting information through communication channel this research planned to provide the solution for hiding or revolving and securing information without any distortion in source image. The resultant image is exactly same as the source image that means number of pixel in the decoded image is same as number of pixels in the original secret image.

The proposed methodology can be design and implemented in following manner:

Phase 1:- Original image / Convert letter into Image.

At the first stage of methodology, we take an image that we want to send or if we want to send letter document then it must necessary to convert that letter into an image format or we may embed the textual information into the image as shown in Fig.3 below

Fig.3:- Source Image / Original Image

Phase 2:- Splitting Original Image into Encrypted Share 1 and Share 2.

After selecting the source image, during the Phase 2 proposed methodology encrypt that source image / Original image into two parts called as Share. After splitting the original image we got two Shares such as Share 1 and Share 2 as shown in following fig.4. These Shares are in encrypted form that means any one cannot able to see the original contents of the image. Hence now the original contents of image are converted into encrypted form (Cipher form) so that it is not possible to read it normally through human eye. All the original contents of source image now split-up into two Shares in distorted form.

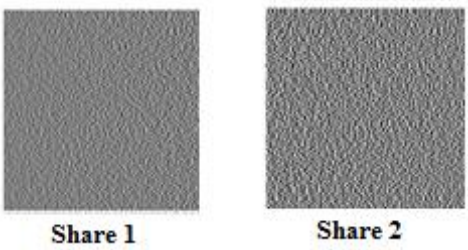

Fig.4:- Encrypted Share 1 and Share 2

Phase 3:- Convert Encrypted Share 2 into Cells.

Fig.5:- Encrypted Share 2

At the edge of Phase 3, out of the two Shares, we select the second Share 2 as shown in Fig.5 and convert it into sub-shares called as Cells. After converting Share 2 into the Cell form, the Share 2 is now converted into the tiles. Each tile involves collection of pixels associated with the referenced Cell and these Cells also have their indexed number. The converted Share 2 into Cells form Share 2 is shown in following fig.6.

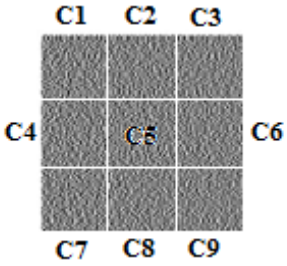

Fig. 6:- Encrypted Cell formed Share 2

Phase 4:- Shuffle the Cells of Share 2 and Generate Key.

Now in Phase 4, all Cells of Share 2 are shuffles so that cells are arranged in disordered form as shown in Fig.7. In this phase again we give more strength to encrypted Share 2, due to which unauthorized user or hacker are not able to find original dimensions of Cell and neither able arranged all Cells in proper order. After disordering all Cells of Share 2, sequence of disorder Cells of encrypted Share 2 is used to generate the Key, which is helpful in future to arrange the Cells of encrypted Share 2 during the decryption process.

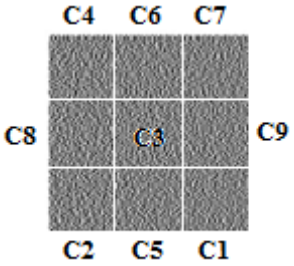

Fig. 7:- Encrypted Cell Shuffled Share 2

Phase 5:- Send encrypted Cell Shuffled Share 2 and Key towards Participants.

In the Phase 5, Secret Key and encrypted Cell Shuffled Share 2 will be sends towards the participant at receiver side through different communication channels. Phase 5 only responsible for sending secret Key and encrypted Cell Shuffled Share 2 towards recipients.

Phase 6:- Rearrange all Shuffled Cells in sequence to form Share 2 by using secret Key.

At Phase 6, all Shuffled Cells of encrypted Share 2 are rearranged in original sequential form so that disordered form of encrypted Share 2 gets converted into the original sequential form. The secret Key is essential thing which play vital role to convert encrypted Shuffled Cells of Share 2 into its proper sequence as shown in Fig.8.

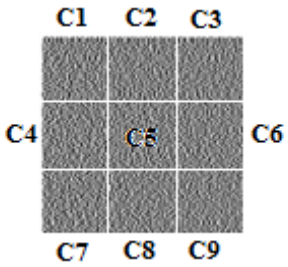

Fig. 8:- Rearrange all Shuffled Cells of encrypted Share 2

At the Receiver side, Receiver use a secret key (Symmetric key) for re-arranging shuffled Cells (Sub-Shares / tiles) gets arranged into a proper sequence as that of in original image (Source image) so that cipher image is converted into a source image (Original image).

Phase 7:- Superimpose Transparencies of Share 1 and Share 2 to reveal Original Image.

The Phase 7 is the last phase of the methodology in which encrypted Share 2 is superimposed with encrypted Share 1. As encrypted Share 2 is stacked with the encrypted Share 1, the original source image get reveal without any computation through human eye. This is a decryption process. The decryption also applicable to revolve information hides in a resultant image as shown in Fig.9.

Fig. 9:- Source Image reveal after Superimposing Share 1 with Share 2

5. Importance of study / Society application:

Visual Cryptography [3] is a secret sharing technique which facilitates the security of information. It neither requires complex encryption, decryption algorithms nor large amount of computing power to retrieve the secret information.

There are many applications of proposed research used for the society which are described as below:

- **International status.**

Provide security to visual images is one of the most important issues discussed worldwide. The Visual Cryptography used to authenticate the document embedded with a copyright share, which is not visible to naked eyes. But when overlapped with the corresponding share reveals the copyright information. The purpose of visual cryptography is to hide the data from a third party.

- **National Status**

Visual Cryptography (VC) is a wide area of proposed research used in data hiding, securing images, color imaging and other such fields. Visual Cryptography and secure comes in the field of confidential data hiding used in Indian cybercrime. Indian Cyber security experts use cryptography to design algorithms, ciphers, and other security measures that codify and protect Indian companies and Indian customer data.

The technique of Visual Cryptography in images has its scope on transmission of data in highly secured manner through communication channel. It is used in many fields for transferring and hiding data in secure manner in defense, financial sectors, Indian Government higher level offices, intelligence agencies etc.

- **Significance of the study**

The proposed Visual Cryptography Scheme and Secure Secret Sharing Scheme reduce the total time which is required for communicating, maintaining, transferring and developing information security and applicable for following purposes…

1. Secret Communication
2. Copyright Protection
3. Secret data storing
4. Document Authentication

6. Proposed work Plan / Formulation and Structure of Study:

Tentative phase wise plan of proposed study are to be designed based on work distribution accomplish during the development of this research.

- **Phase 1:**
    1. To provide the overview of the Visual Cryptography (VC) and Secret Sharing Scheme (SSS) based on the previous related work.
    2. To provide the efficient and more accurate solutions to various problems and different challenges related to Visual Cryptography (VC) and Secret Sharing Scheme (SSS).
- **Phase 2:**
    1. To design and implement a new approach in Visual Cryptography (VC) Scheme in order to secure an image transmission and generate Shares.
    2. Minimize and remove the problems occurred during this phase.
- **Phase 3:**
    1. To design and implement a new approach in Secret Sharing Scheme (SSS) in order to accomplish hide data, encrypt data as well to transmit encrypted data securely.
    2. Minimize and remove the problems occurred during this phase.
- **Phase 4:**
    1. Implement a new approach in Visual Cryptography (VC) to assemble the Shares into the stack so as to reveal distortion free image
    2. Minimize and remove the problems occurred during this phase.
- **Phase 5:**
    3. To evaluate and analyze the performance of proposed Visual cryptography scheme and Secure Secret Sharing Scheme so as to clarify its efficiency in comparison to recent related work.
    4. Improve the quality of resultant image and data hiding or revolving efficiency by applying some error diffusion technique.
- **Phase 6:**
    1. To enlist some of the application of newly developed scheme.
    2. To contribute the commendation and assumption for the future development.
    3. Report writing.

7. References:

1. ***Cryptography is the science of protecting information by transforming it into a secure format. It aims at ensuring high end communication between the sender and receiver without any loss of information [1].*** D.C.Mishra, R.K.Sharma, Rakesh Ranjan, M. Hanmandlu. **Optik 126 (2015) 3812–3822, s.l. : Optik Elsevier, 2015.**

2. ***Visual cryptography for color images.*** Hou, Young-Chang. **s.l. : PERGAMON, 2003, Vols. Pattern Recognition 36 (2003) 1619 – 1629.**

3. ***Image sharing method for gray-level images.*** Chen, Wei-Kuei. **2013, Vol. The Journal of Systems and Software 86 (2013), pp. 581– 585.**

4. ***Safeguarding cryptographic keys.*** BLAKLEY, G. R. **s.l. : Proc. of National Computer Conference, 1979, 1979, Vols. 48,, pp. 313-317.**

5. ***How to Share a Secret.*** Shamir, Adi. **s.l. : Communications of the ACM 22(11), pp. 612-613.**

6. ***Secret Sharing Schemes using Thresholding.*** Abhishek Mishra, Ashutosh Gupta. **s.l. : IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS, Jan-Feb 2016, Vols. Vol.6, No1, Jan-Feb 2016. ISSN: 2249-9555.**

7. Cimato, S., Yang, C.N.[Eds]. ***Visual Cryptography and secret image sharring.*** **s.l. : CRC Press, 2011.**

8. ***A Survey of Various Cryptography Techniques.*** Azmat Khan, Danilsh Ali. **1, s.l. : International Journal of Computer Science (/ijCS Journal), 2016, International Journal of Computer Science (/ijCS Journal), Vol. 4, pp. 2, 660-665.**

9. ***" Visual cryptography".*** Shamir, Naor and A. **s.l. : Advances in Cryptology EUROCRYPT "94,M Lecture Notes in Computer Science, 1995, Vols. 950,no.7, pp.1–12.**

10. ***"A Study On Visual Cryptography".*** C.C. Wu, L.H. Chen. **Taiwan, R.O.C. : Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.**

11. ***"Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes.".*** Verheul, E. and Tilborg, H. V. **1997. pp. 179–196.**

12. ***"Multi-Secrets Visual Secret Sharing".*** Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei. **s.l. : Proceedings of APCC2008, IEICE, 2008.**

13. ***Image Encryption based on Cell Shuffling and Scanning Techniques.*** Chandra Prakash Singer, Jyoti Bharti, R.K. Pateriya. **October-2017, IEEE : Proceeding International**

Conference on Recent Innovations is Signal Processing and Embedded Systems, 2017, Vols. RISE-2017, pp. 27-29. ISBN 978-1-5090-4760-4/17.

14. ***A NEW VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE USING SLIDING PUZZLE TECHNIQUE.*** Kalyan Das, Aromita Sen, Samir Kumar Bandyopadhyay. **04, s.l. : International Journal of Information Research and Review, April 2016, 2016, Vol. 03, pp. 2238-2241.**

15. ***Design and Implementation of Visual Cryptography System for Transmission of Secure Data.*** Guru Prasad M. Bhat, Nayana G. Bhat. **7, s.l. : International Joournal On Recent and Innovation Trends in Cmputing and Communication, 2017, Vol. 5, pp. 718-721. ISSN 2321-8169.**

16. ***"Visual Cryptography and its Application".*** Hou, Young-Chang. **s.l. : Ventus Publishing Aps, 2012. pp. 1-144.**

17. ***State-of-the-Art Visual Cryptography Schemes.*** Mahmoud E. Hodeish, Dr.V.T. Humbe. **2, s.l. : International Journal of Electronica Communication and Computer Engineering, 2014, Vol. 5. ISSN(Online):22546-071X, ISSN(Print) 2278-4209.**

18. ***Visual Cryptography: A Review.*** Dipesh Vaya, Sarika Khadelwal, Teena Hadpawat. **s.l. : International Journal of Computer Applications, 2017, Vols. 174 - No. 5 September 2017, pp. 0975-8887.**

19. ***DIGITAL DATA SECURITY USING VISUAL CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES: AN EXTENSIVE REVIEW.*** Nandini, Jahnavi S. Dr. C. **9, s.l. : JETIR September 2018, 2018, JETIR September 2018, Vol. 5.**

20. ***Quality Enhancement of Visual Cryptography for Secret Sharing of Binary, Gray and Color Images.*** Ramesh N. Chaturvedi, Sudeep D. Thepade, Swati N. Ahirrao. **s.l. : Fourth International Conference On Computing Communication Control and Automation (ICCUBEA), 2018, IEEE , Vols. 978-1-5386-5257/18.**

21. ***Visual Cryptography using Half-toned Colored Images.*** Afshan Mohammadi, Dr. Jalesh Kumar. **08 Aug 2020, s.l. : International Research Journal of Engineering and Technology (IRJET), 2020, International Research Journal of Engineering and Technology (IRJET), Vol. 07.**

22. ***An Efficirent(n,n) Visual Secret Image Sharing using Random Grids with XOR Recovery.*** Ram Gopal Sharma, Dr. Hitendra Garg, Dr. Priti Dimri. **DOI: 10.5815/ijcnis., s.l. : Onine November 2019 in MECS, 2019.**

23. ***A (2,2) Secret Sharing Scheme for Visual Cryptography without Pixel Expansion.*** Mahmoud E. Hodeish, Dr.V.T.Humbe. **s.l. : IEEE International Conference On Electronics, Signals, Communication and Optimization (EESCO) - 2015, 2015, IEEE International Conference On Electronics, Signals, Communication and Optimization (EESCO) - 2015, Vols. 978-1-4799-7678-2.**

24. ***A Novel image Encryption Algorithm using AES and Visual Cryptography.*** Venkata Krishna Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni. **s.l. : IEEE International Conference On Next Generation Computing Technologies (NGCT) - 2016, 2016, IEEE International Conference On Next Generation Computing Technologies (NGCT) - 2016, Vols. 976-1-5090-3257-0/16.**

25. ***Visual Cryptography.*** Rajkumar Kushwaha, Ankit Gajakosh, Prasanna More. **1, s.l. : IJCRT, 2018, IJCRT, Vol. 6. ISSN: 2320-2882.**

26. ***An Optimal(k,n) Visual Secret Sharing Scheme for Information Security.*** Mahmoud E. Hodeish, Linas Bukauskas, Dr. Vikas T. Humbe. **s.l. : Procedia Computer Science 93, 2016, ELSEVIER, pp. 760-767.**

27. ***Encryption and Decryption of Color Images using Visual Cryptography.*** M.Karolin, Dr.T.Meryyappan,SM.Thamarai. **s.l. : International Journal of Pure and Applied Mathematics, 2018, International Journal of Pure and Applied Mathematics, Vol. 118 No. 8 2018, pp. 277-281. ISSN:1311-8080(Printed version ISSN:1314-3395(Online version).**

28. ***A Robust Visual Cryptography Technique for Photographic Grayscale Image Using Block Optimization and Blind Invisible Watermarking.*** Ayan Banerjee, Sreya Banerjee. **s.l. : International Journal of Computer Theory and Engineering, 2012, Vols. 4, No 2 April 2012.**

29. ***Database security Using Multi-Share Visual Cryprography.*** Dr. G.D. Dalvi, Dr. Mrs. S.D. Wakde, Prof. P.V.Kale. **2, s.l. : IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), 2019, Vol. 14, pp. 37-43.**

30. ***A Novel Two Stage Binary Image security System Using(2,2) Visual Cryptography Scheme.*** Mr. Rohit S., Mr.Vinay G. **3, s.l. : IJCER, 2012, Vol. 2, pp. 642-646.**

31. ***A Visual Cryptgrahic Technique to Secure Image Shares.*** Jagdeep Verma, Dr.Vineeta Khemchandani. **1, 2012, International Journal of Engineering Research and Application (IJERA), Vol. 2, pp. 1121-1125. ISSN: 2248-9622.**

32. ***Image Encryption and decryption using RSA Algorithm with Share Creation Techniques.*** M.Karolin, T. Meyyappan. **2, s.l. : Blue Eyes Inteligence Engineering & Sciences Publication, 2019, International Journal of Engineering and Advanced Technology(IJEAT), Vol. 9. ISSN:2249-8958(Online).**

33. ***Implementation of Encrypted Visual Cryptographic Shares using RSA algorithm on FPGA.*** Manojkumar G.L., Subramanyam M. **s.l. : International Journal of Engineering Research & Technology(IJERT) NCRTS 14 Conferenc Proceedings, 2014, International Journal of Engineering Research & Technology(IJERT) NCRTS 14 Conferenc Proceedings. ISSN: 2278-0181.**

34. ***New Fool Proof Examination System through Color Visual Cryptography and Signature Authentication.*** Mohamed Fathimal, Arockia Jansirani. **Janyary 2019, s.l. : The International Arab journal of Information Technology, 2059, Vol. 16 No. 1.**

35. ***Construction of Basic Matrices for(k,n) and Progressive Visual Cryptography Schemes.*** S.B.Bhagate, P.J.Kulkarni. **1, Feb 2018, s.l. : JCSE Internatinal Journal of Computer Sciences and Engineering, 2018, Vol. 6. E-ISSN:2347-2693.**

36. ***A Visual Crypt stego Approach with Randomized Puzzle Block Generation for Highest Secret Sharing.*** Dr.D.Devakumari. **11 November 2017, s.l. : Journal of Network Communication and Engineering Technologies (JNCET), 2017, Vol. 7. ISSN: 2395-5317.**

37. ***A Simple Scheme for Visual Cryptography.*** Das, Mihir. **4, s.l. : International Journal of Computer and Communication Technology, October 2010, International Journal of Computer and Communication Technology, Vol. 1.**

38. ***An Effective Multi-Level Multi-shares Visual Cryptography Technique.*** Gopal D. Dalvi, Dr.S.D.Wakde, P.V.Kale. **s.l. : 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, IEEE.**

39. ***Image encryption by multiple random grids.*** Shyu, Shyong Jian. **s.l. : ELSEVIER, 2009, Vol. Pattern Recognition 42 (2009), pp. 1582-1596.**

40. ***Image ecryption by random grids.*** Shyu, Shyong Jian. **s.l. : ELSEVIER, 2007, Vol. Pattern Recognition 40 (2007), pp. 1014-1031.**

Signature	**Signature**
Mr. Anil B. Alde	**Dr. Vikas T. Humbe**
Research Scholar	Research Supervisor / Guide